Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 80 (2014) 437 – 444

Procedia Engineering

www.elsevier.com/locate/procedia

3rd International Symposium on Aircraft Airworthiness, ISAA 2013

Implication of mishaps to preliminary hazard analysis of hypersonic vehicles

Lei GONG[a,b], Shuguang ZHANG[a,b,*], Peng TANG[a,c], Yang FENG[a,b]

[a]*Airworthiness Technology Research Center, National Laboratory for Aeronautics and Astronautics, Beihang University, 37 Xueyuan Road, Beijing 100191, P.R. China*

[b]*School of Transportation Science and Engineering, Beihang University, 37 Xueyuan Road, Beijing 100191, P.R. China*

[c]*School of Energy and Power Engineering, Beihang University, 37 Xueyuan Road, Beijing 100191, P.R. China*

Abstract

To highlight the safety-critical areas of hypersonic vehicles through data-driven analysis, this paper applies the hazardous factors of the Preliminary Hazard Analysis (PHA) method recommended in the advisory circular AC-431.35-2A to review 99 mishap flights of hypersonic vehicles. Mishaps with complex processes are modeled and analyzed using a new graphic method for aviation accident analysis named accident tree (AcciTree). Unsafe factors identified are then examined statistically to highlight the safety-critical zones and to identify possible new hazardous factors for the PHA list. The results indicate that the first-level categories of the PHA list have been defined extensive enough by the method to cover all hazardous factors examined in the 99 mishaps; and six factors are newly identified as supplements to the second-level categories to address the hypersonic features. The top six hazardous factors are system malfunction, hazardous component, protective system, system compatibility, undesired state, and human error; and the six systems with top high occurrence frequencies are propulsion, heat protection, flight control, brake, environment control, and landing gear.

Selection and peer-review under responsibility of Airworthiness Technologies Research Center, Beihang University/NLAA.

Keywords: Hypersonic; Hazard identification; Preliminary hazard analysis; Accident analysis; Hazardous Factor

Nomenclature

* Corresponding author. Tel.: +86-10-82315237; fax: +86-10-82315237.

E-mail address: gnahz@buaa.edu.cn.

Selection and peer-review under responsibility of Airworthiness Technologies Research Center, Beihang University/NLAA.

doi:10.1016/j.proeng.2014.09.102

F_r	relative occurrence frequency of a system factor
N_O	occurrence number of a system factor
N_A	applicable mishap number of a system factor

1. Introduction

Increasing activities in space transportation have led to efforts of authorities to regulate this area. The European Aviation Safety Agency (EASA) has proposed to accommodate sub-orbital and orbital flights in the regulation [1]. And, the Federal Aviation Administration (FAA) has established a regulation system to address safety aspects of commercial space transportation [2]. In the Federal Aviation Regulation (FAR) system, one important focus of certification is on system safety process of the proposed mission; and, the beginning of the system safety process lies in hazard identification [2-3].

Preliminary Hazard Analysis (PHA) is one of the methods recommended by the FAA in advisory circular AC-431.35-2A for hazard identification in system safety processes of reusable launch and reentry vehicles [3]. Different from the Functional Hazard Analysis (FHA) widely used in aviation industry [4], the PHA adopts a list of hazardous factors as guides and minimum considerations for identification of hazards from proposed missions [5]. However, within this scope, which factors are relatively more safety-critical? How well could the factors cover the causes of existing mishaps? Answers to these questions may trace back to data-driven studies for the safety-critical zones of these vehicles.

Based on the hazardous factors of PHA, 99 mishap flights of hypersonic vehicles are studied in this paper to highlight the safety-critical areas and identify possible new hazardous factors for the PHA list through data-driven analysis.

2. Unsafe factors of the PHA

In the PHA list, hazardous factors are divided into two levels. The first level provides general hazardous categories, and the second puts forward detailed sub-categories. The hazardous factors of PHA given in Ref. [5] are summarized as follows.

(1) Hazardous components: energy sources, fuels, propellants, explosives, pressure system, etc.
(2) Subsystem interfaces: signals, voltages, timing, human interaction, hardware, etc.
(3) System compatibility constraints: material compatibility, electromagnetic interference, transient current, ionizing radiation, etc.
(4) Environmental constraints: drop, shock, extreme temperature, noise and health hazards, fire, electrostatic discharge, lightning, X-ray, electromagnetic radiation, laser radiation, etc.
(5) Undesired states: inadvertent activation, fire/explosive initiation and propagation, failure to safe, etc.
(6) Malfunctions to the system, subsystems, or computing system.
(7) Software errors: programming errors, programming omissions, logic errors, etc.
(8) Operating, test, maintenance, and emergency procedures.
(9) Human error: operator functions, tasks, requirements, etc.
(10) Crash and survival safety: egress, rescue, salvage, etc.
(11) Life-cycle support: demilitarization/disposal, explosive ordnance disposal, surveillance, handing, transportation, storage, etc.
(12) Facilities, support equipment, and training.

(13) Safety equipment and safeguards: interlocks, system redundancy, fail-safe design, subsystem protection, fire suppression systems, personal protective equipment, warning labels, etc.
(14) Protective clothing, equipment, or devices.
(15) Training and certification pertaining to safe operation and maintenance of the system.
(16) System phases: test, manufacture, operations, maintenance, transportation, storage, disposal, etc.

3. Data sources and analysis methods

3.1. Data sources

Only mishaps of hypersonic vehicles which are severer than the critical level are included for this study, i.e., mishaps severer than "*major property damage to the public, major safety-critical system damage or reduced capability, significant reduction in safety margins, or significant increase in crew workload*", as defined in AC-437.55-1 [6]. The mishap cases are from public reports, with a total of 99 mishaps of 8 programs, including X-15 [7-8], DC-X(A) [9], Space Shuttle [10-12], X-37 [13-14], HyFly [15], X-43A [16-17], X-51A [18] and HTV-2 [19].

3.2. Analysis methods

To the mishaps with direct and simple causes, the conclusions given in the reports are directly categorized according to the PHA list [5]. However, in some cases like the space shuttle Challenger disaster [11] and the X-15 reentry breakdown [7-8], the accident processes and causes are complex, involving adverse interactions among human, technology, and environment, as well as organizational deficiencies. These mishaps are analyzed using a new accident analysis approach named Accident Tree (AcciTree) [20] to identify latent hazardous factors from the investigation information as supplements to the official conclusions.

AcciTree is an integrated graphic-taxonomic method which adopts a Y-shaped structure with a reaction-based concept for modeling the adverse human-aircraft-environment interactions of the accident direct process, and uses hierarchical levels for modeling the evolvement of the organizational deficiencies. To reduce the discrepancies of analysis due to entire subjectivity of the graphic method [21-25], further integration of the well-established Human Factors Analysis and Classification System (HFACS) [26] into the graphic model establishes guides and minimum considerations for the graphic modeling, which enhances both reliability of the graphic analysis and logicality of the taxonomic analysis, thus improves the completeness of the results [20].

As a demonstration, the X-15 reentry breakdown accident [7-8] is analyzed by AcciTree method as follows.

On November 15, 1967, an U.S. Air Force test pilot lost his life while flying the rocket-powered X-15 research vehicle in a parabolic space flight profile. Investigation revealed that the primary cause was loss of mode awareness due to misinterpretation of a dual-use flight instrument – the confusion between yaw and roll indications led to inappropriate flight control input and subsequent loss of control of aircraft. Other contributive factors include system failures, pilot's spatial disorientation, oculoagravic illusion due to high axial acceleration, and flawed ground monitoring system design [7-8]. AcciTree model of the X-15 accident is shown in Fig. 1.

As shown in Fig. 1, the three sectors of the Y-shaped accident direct model – human, aircraft, and environment – provides convenience for describing both the interactions and the boundaries between any two parts of the three sectors. Unsafe events within the Y-shaped structure are linked by reaction chains, and the whole accident direct process is described by a spiral reaction network converging at the accident.

The organization model adopts a cause-consequence mechanism and consists of three levels including unsafe supervisions, organizational influences of company, as well as regulatory failures and legislation deficiencies.

Factors newly identified from the AcciTree analyses are also categorized according to the PHA list [5].

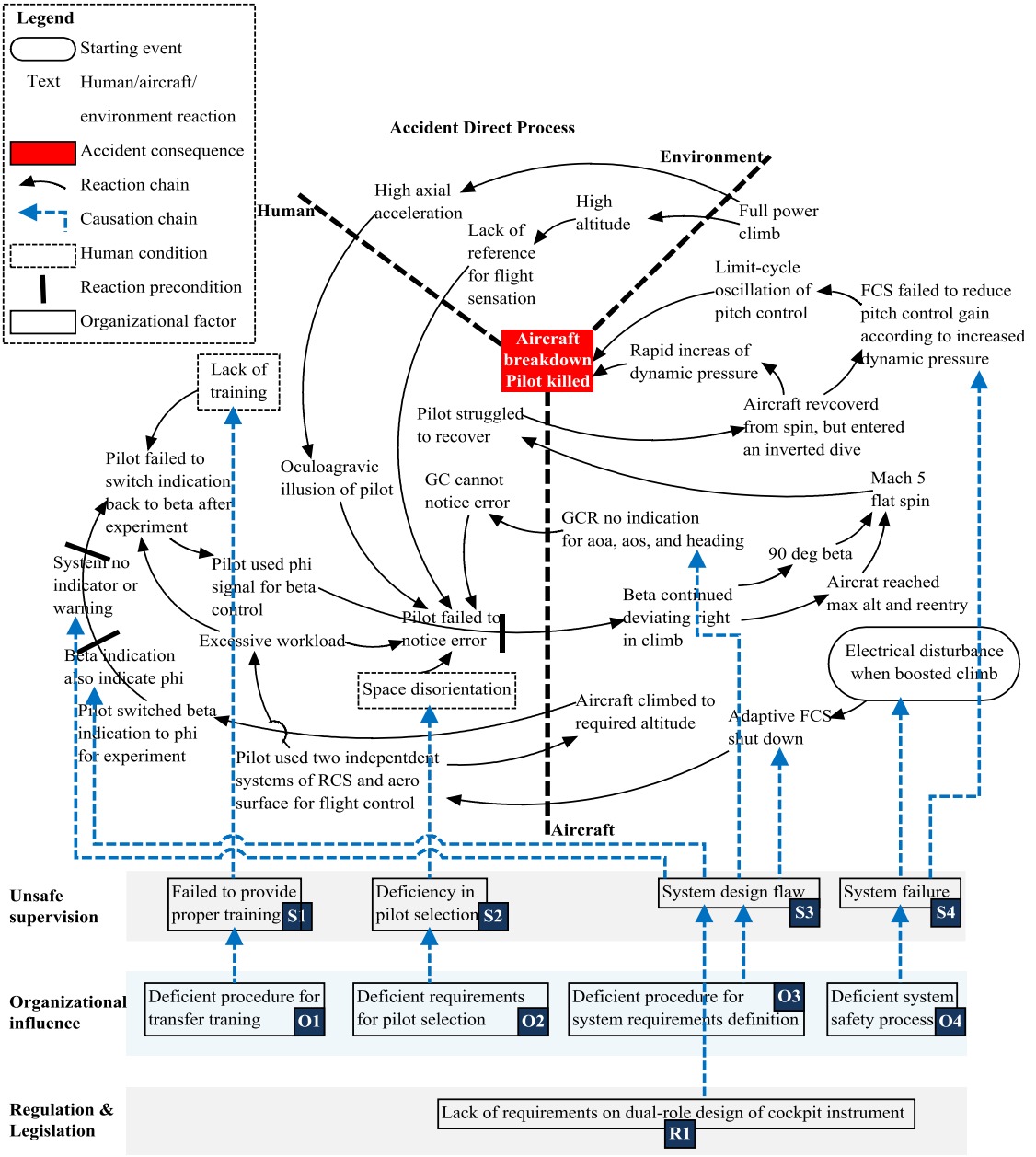

Fig. 1 AcciTree model of the X-15 reentry breakdown accident. First letters of the numbers of organizational factors -- “S”, “O” and “R” -- refer to the “Supervisory”, “Organizational” and “Regulation & Legislation” levels.

3.3. Statistical methods

The top 6 categories of the statistic result are further analyzed using second-level sub-categories of the PHA list [5]. If factors identified above cannot be covered by the PHA list [5], appropriate new categories are developed and designated to these factors.

The mishaps are also analyzed according to system types to highlight the safety-critical systems. Relative occurrence frequency of a system factor, F_r, is defined as follows:

$$F_r = \frac{N_O}{N_A} \tag{1}$$

Where N_O is the occurrence number of a system factor; and N_A is the applicable mishap number of the factor. Applicable mishap of a factor is defined as a mishap that involves the factor.

4. Results

The results of the hazardous factors-based analysis are shown in Fig. 2 (a), and the results of the system-based study are given in Fig. 2 (b). The top 6 categories of the hazard-based analysis are further examined in Table 1, in which items in grey background are hazardous factors newly identified from the hypersonic mishaps.

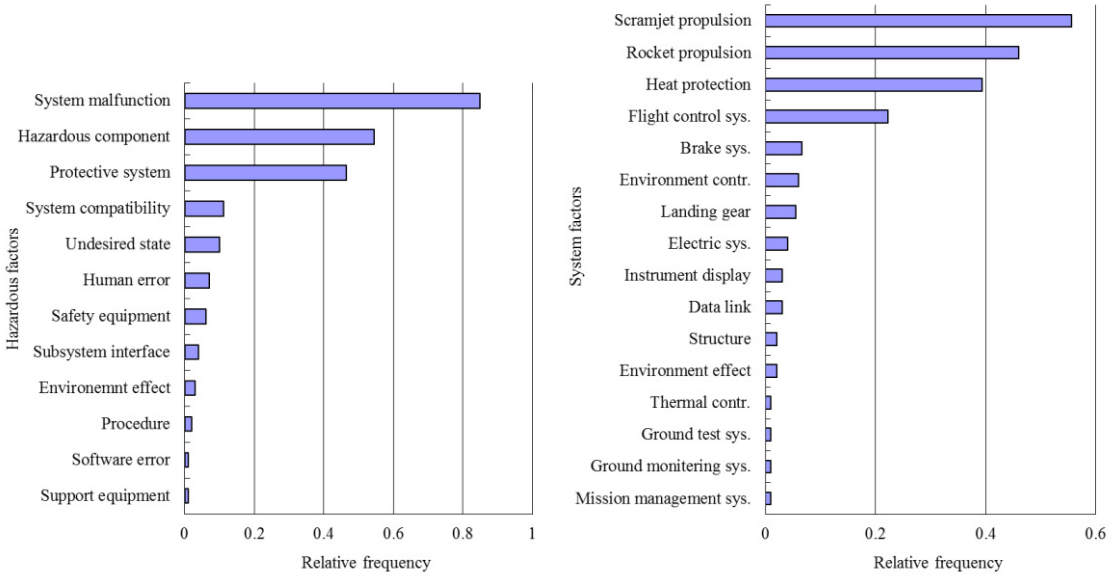

Fig. 2. (a) result of the hazardous factors-based analysis; (b) result of the system-based analysis

Table 1. Sub-category distribution of the top 6 categories in hazardous factors-based analysis. Items in grey background are hazardous factors newly identified from the hypersonic mishaps

Categories	Sub-categories	Ratios (%)
System malfunction	Mechanical	56.0
	Electric-Mechanical	29.8

	Electronic	10.6
	Electric	3.6
Hazardous component	Fuel	42.6
	Propulsive system	40.7
	Pressure system	16.7
Protective system	Heat protection	87.0
	Environment control	13.0
System compatibility	Hazardous factors interference	45.4
	Control algorithm	36.4
	System principle	9.1
	Electric interference	9.1
Undesired state	System anomaly	50.0
	Exploration of new technology	40.0
	Time delay	10.0
Human error	Skill-based error	42.8
	Conceptual error	14.3
	Adverse physiological state	14.3
	Physical limitation	14.3
	Adverse mental state	14.3

The analysis indicates that all unsafe factors in the 99 mishaps examined are covered by the first-level categories of the PHA list [5]. However, the second-level sub-categories of the PHA list cannot cover all mishaps factors. For example, in the "system compatibility constraints" category, the incompatibility between flight control algorithm and flight dynamics characteristics of vehicle, as observed in the X-43A mishap [17], is not covered by the PHA sub-categories. The incompatibility of system principles between engine system and ground test system, as observed in the X-15 ground test explosion [7] is not covered by the sub-categories either. Therefore, it is necessary to identify new factors as supplements to the PHA sub-categories to address these hypersonic mishap factors. The factors newly identified include:

- Heat protection for the protective system category.
- Hazardous factors interference, control algorithm, and system principle for the system compatibility category.
- Exploration of new technology and time delay for the undesired state category.

Besides highlighting the safety-critical zones, some interesting findings are also revealed from the statistic results:

- In the system malfunction category, the electronic and electric components, which are often considered more prone to failures, have far lower ratios than the mechanical components in the severer-than-critical mishaps. This is probably due to the extensively-used redundant design for electronic and electric parts of modern aerospace system, which effectively decreases the possibility of single failure causing hazardous effects and makes the mechanical failures relatively prominent.
- In view of protective system, the heat protection issue, which is observed in multiple mishaps including X-15 [7], Space Shuttle [10] and HTV-2 [19], and constitutes 87% of all protective system issues, is critical for flight safety of hypersonic vehicles.
- While exploring one of the most cutting-edge areas of aerospace, the less-understood features of the hypersonic flight and the novel technologies adopted inevitably poses potential risks. One of the significant risks is the new flight dynamics characteristics emerging in the hypersonic flight, which

caused catastrophic mishaps of several recent vehicles, including the breakdown of X-43A in 2001 caused by lateral-directional divergence due to model uncertainty [17], and the reentry divergence and following self-destruction of HTV-2 in 2010 due to unknown aerodynamic characteristics of hypersonic phase [19]. Since flight control directly affects flight safety, it is necessary to pay special attentions to the new flight dynamics and control mechanisms possibly emerging in hypersonic phase to reduce the flight risk.

5. Conclusions

(1) With a structure of two-level categories in PHA, the first-level categories have been defined extensive enough by the method, and can cover all hazardous factors examined in the 99 mishaps. While the second-level sub-categories show to be insufficient for hypersonic vehicles. Six more factors are identified from the mishaps, and hence taken as supplements to the second-level categories.

(2) The six systems with top high occurrence frequencies in severer-than-critical mishaps are propulsion, heat protection, flight control, brake, environment control, and landing gear. The six categories of top hazardous factors are system malfunction, hazardous component, protective system, system compatibility, undesired state, and human error.

(3) It is found that in the "exploration of new technology" sub-category, special attentions need to be paid to the new flight dynamics and control mechanisms possibly emerging in hypersonic phase to reduce flight risks.

References

[1] Marciacq J-B. Accommodating Sub-orbital and Orbital (SOA) Flights in the EU. *6th IAASS Conference*, Montreal, Canada; 2013.

[2] Code of Federal Regulations, Part 431, *Launch and Reentry of a Reusable Launch Vehicle (RLV)*. Washington, D.C: Federal Aviation Administration.

[3] AC-431.35-2A, *Reusable Launch and Reentry Vehicle System Safety Process*. Washington, D.C: Federal Aviation Administration; 2005.

[4] SAE ARP-4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Warrendale: Society of Automotive Engineers; 1996.

[5] Ericson CA. *Hazard Analysis Techniques for System Safety*. Hoboken: John Wiley & Sons, Inc.; 2005, p. 73-93.

[6] AC-437.55-1, *Hazard Analysis for the Launch or Reentry of a Reusable Suborbital Rocket under an Experimental Permit*. Washington, D.C: Federal Aviation Administration; 2007.

[7] Jenkins DR. *Hypersonics before the Shuttle: A Concise History of the X-15 Research Airplane*. NASA SP-2000-4518. Washington, D.C: National Aeronautics and Space Administration; 2000.

[8] Merlin PW, Bendrick GA, Holland DA. *Breaking the Mishap Chain: Human Factors Lessons Learned from Aerospace Accidents and Incidents in Research, Flight, Test, and Development*. NASA SP-2011-594. Washington, D.C: National Aeronautics and Space Administration; 2011.

[9] The Delta Clipper Experimental: Flight Testing Archive. Available from:
http://www.hq.nasa.gov/pao/History/x-33/dc-xa.htm

[10] Legler RD, Bennett FV. *Space Shuttle Missions Summary*. NASA/TM-2011-216142. Washington, D.C: National Aeronautics and Space Administration; 2011.

[11] Rogers WP, Armstrong NA, Acheson DC, et al. *Report of the Presidential Commission on the Space Shuttle Challenger Accident*. Presidential Commission on the Space Shuttle Challenger Accident; 1986.

[12] Gehman HW Jr, Barry JL, Deal DW, et al. *Columbia Accident Investigation Board Report Volume 1*. Columbia Accident Investigation Board; 2003.

[13] Grantz AC. X-37B Orbital Test Vehicle and Derivatives. *AIAA SPACE 2011 Conference & Exposition*, AIAA-2011-7315; 2011.

[14] David L. X-37 Flies at Mojave but Encounters Landing Problems. Available from:
http://www.space.com/2267-37-flies-mojave-encounters-landing-problems.html

[15] Hypersonics Flight Demonstration Program (HyFly). Available from:
http://www.globalsecurity.org/military/systems/munitions/hyfly.htm

[16] Peebles C. The X-43 Fin Actuation System Problem – Reliability in Shades of Gray. *AIAA SPACE 2006 Conference & Exposition*, AIAA-2006-7469; 2006.

[17] Hughes RW, Lackovich JJ Jr, Bauer FH, et al. *Report of Findings X-43A Mishap*. X-43A Mishap Investigation Board; 2003.

[18] Warwick G. Fin Failure Dooms Third X-51A Flight. Available from:
http://www.aviationweek.com/Article.aspx?id=/article-xml/awx_08_15_2012_p0-486354.xml

[19] Majumdar D. DARPA's HTV-2 Crashed Because It Blew Off Chunks. Available from:
http://www.flightglobal.com/blogs/the-dewline/2012/04/darpas-htv-2-crashed-because-i.html

[20] Gong L, Zhang SG, Tang P, et al. An Integrated Graphic-Taxonomic-Associative Approach to Analyze Human Factors in Aviation Accidents. *Chinese Journal of Aeronautics* (in peer review)

[21] Salmon PM, Cornelissen M, Trotter MJ. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. *Safety Science* 2012; **50**(4): 1158-70.

[22] Svedung I, Rasmussen J. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. *Safety Science* 2002; **40**(5): 397-417.

[23] Leveson NG. A new accident model for engineering safer systems. *Safety Science* 2004; **42**(4): 237-70.

[24] Saleh JH, Marais KB, Bakolas E, et al. Highlights from the literature on accident causation and system safety: review of major ideas, recent contributions, and challenges. *Reliability Engineering and System Safety* 2010; **95**(11): 1105-16.

[25] Debrincat J, Bil C, Clark G. Assessing organisational factors in aircraft accidents using a hybrid Reason and AcciMap model. *Engineering Failure Analysis* 2013; **27**: 52-60.

[26] Wiegmann DA, Shappell SA. *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*. Hants, England: Ashgate Publishing Limited; Vermont, U.S.A.: Ashgate Publishing Company; 2003.